

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

UNITED STATES OF AMERICA	:	CRIMINAL NO. _____
v.	:	DATE FILED: _____
TREYTON DANIEL AUBUCHON a/k/a "Aloel"	:	VIOLATIONS: 18 U.S.C. § 1349 (conspiracy to commit wire fraud – 1 count) 18 U.S.C. § 1343 (wire fraud – 1 count) 18 U.S.C. § 1028A (aggravated identity theft – 1 count) Notice of Forfeiture

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES THAT:

At all times material to this Indictment:

Relevant Individuals, Entities, and Definitions

1. Defendant TREYTON DANIEL AUBUCHON, a/k/a "Aloel," was a resident of the State of Wisconsin.
2. Ruben Filipe Gabriel Martins, a/k/a "Feepsy," charged elsewhere, was a resident of the United Kingdom.
3. Victim 1 was a resident of, and present in, the Eastern District of Pennsylvania.
4. "Cryptocurrency" was a class of financial instruments that allowed the transfer of value between individuals without any third-party mediation or government regulation. Cryptocurrencies existed entirely in digital format and not in any physical form. Such cryptocurrency was not issued by any government, bank, or company, but rather was generated and controlled automatically through computer software operated on a decentralized, "peer-to-

peer” network sometimes using the “Blockchain” concept. The Blockchain for cryptocurrencies was the record of every transaction that had ever occurred in that particular cryptocurrency. It was often referred to as a “ledger” of all transactions. This transfer of cryptocurrency was accomplished with a set of cryptographic protocols. These protocols required that each transaction’s sender and receiver held an appropriate cryptographic key. Examples of cryptocurrencies in widespread use included Bitcoin, Ethereum, and Litecoin.

5. Cryptocurrencies were traded on cryptocurrency exchanges or marketplaces, where users could buy, sell, and trade cryptocurrencies. These exchanges were entirely digital, and transactions were typically performed over the Internet. Some cryptocurrency exchanges allowed direct conversions of cryptocurrencies into government-backed currencies such as U.S. dollars, while other exchanges only allowed buying, selling, and trading of cryptocurrencies.

6. A “seed phrase” is a sequence of random words that stores the data required to access or recover cryptocurrency. Seed phrases are usually generated by cryptocurrency wallets and can be used to recover the contents of the wallet (including virtual currency addresses and private keys). Anyone who possesses the seed phrase can reconstitute the wallet and see and manipulate its contents, including moving them to new addresses.

7. “Social engineering” is a type of fraud scheme wherein individuals call a potential victim and “socially engineer,” or trick them into providing passwords, pins, and other personal information that the callers use to gain unauthorized access to the victim's private accounts, including cryptocurrency accounts, email accounts, bank accounts, and other valuable personal files.

8. A “caller” is the name commonly used for the individuals involved in social engineering schemes who place calls to potential victims and falsely portray themselves as

representatives of cryptocurrency exchanges or online account providers. Their goal is to give the victim enough confidence in their character that the victim will provide access to their online accounts.

9. A “phishing panel” is a tool that cybercriminals use to run phishing attacks and collect data from victims. Phishing panels are hosted on the criminal’s infrastructure. A phishing panel typically has two parts: a “phishing page” and an “administrator panel.” The phishing page is what the victim sees, and is designed to look like a legitimate website, such as a cryptocurrency exchange platform login page. The administrator panel is only accessible to the criminal actor, and it allows them to monitor the phishing attack and take actions. When a victim enters their information into the phishing page, the criminal receives and can view the sensitive information, such as a password entered by a victim, on the admin panel.

10. The “CryptoChameleon Phishing Panel” is a phishing panel used by members of the conspiracy to unlawfully obtain funds, primarily cryptocurrency, from its victims. The CryptoChameleon Phishing Panel employs phishing panels and spoofed domains that mimic the sign-on pages for cryptocurrency companies and exchanges, and other providers of online services, such as email providers. There is the administrator of the CryptoChameleon Phishing Panel. Users of the CryptoChameleon Phishing Panel are given a unique user ID and password. Once granted access to the CryptoChameleon Phishing Panel, users are provided with an admin domain, which generally mimics the name of a cryptocurrency exchange, from which to log-in to the CryptoChameleon Phishing Panel. Users are also granted access to a specific subset of phishing panel domains which they can deploy against victims. The phishing panel domains mimic the legitimate domains of cryptocurrency exchanges, financial institutions, and providers of other online accounts and services. The administrator and the user of the panel are able to

monitor both actions taken by the user and by the victims. The administrator charged a fee to use the CryptoChameleon Phishing Panel.

The Conspiracy

11. From at least in or around October 2023 to on or about June 2025, in the Eastern District of Pennsylvania and elsewhere, defendant

TREYTON DANIEL AUBUCHON,
a/k/a "Aloel"

together with Ruben Filipe Gabriel Martins, charged elsewhere, and other individuals known and unknown to the grand jury, conspired to commit an offense against the United States, namely, wire fraud, that is, knowingly and with the intent to defraud, to devise, and to intend to devise, a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and to transmit and cause to be transmitted certain wire communications in interstate and foreign commerce, for the purpose of executing the scheme and artifice, in violation of Title 18, United States Code, Section 1343.

MANNER AND MEANS

It was part of the conspiracy that:

12. The conspirators obtained and collected databases containing personal identifying information of individuals, which they used to identify potential victims who held accounts with cryptocurrency exchanges.

13. The conspirators, including defendant TREYTON DANIEL AUBUCHON and Ruben Filipe Gabriel Martins, obtained a unique UserIDs, passwords, and associated accounts with the CryptoChameleon Phishing Panel.

14. The conspirators, using personal identifying information of legitimate employees of cryptocurrency exchanges, email providers, or other online account providers, contacted victims via text messages, emails, Internet voice calls, and other means of communication purporting to be employees from the cryptocurrency exchanges, email providers, or other online account providers.

15. Using the CryptoChameleon Phishing Panel and other tools, the conspirators placed voice calls, over the Internet, using providers such as Google Voice, to contact victims. The conspirators engaged in social engineering to convince victims that the callers were employees of cryptocurrency exchanges, email providers, or other online account providers.

16. Using the CryptoChameleon Phishing Panel and other tools, the conspirators caused text messages, voice calls, links, and push notifications to be sent to victims which tricked victims into providing account log-in information, passwords, multi-factor authentication codes, seed phrases, and other means of identification to the conspirators.

17. The conspirators used the fraudulently obtained log-in information, passwords, multi-factor authentication codes, seed phrases, and other means of identification to access victims' cryptocurrency accounts at cryptocurrency exchanges, and to access other online accounts belonging to the victims, and transferred the victims' cryptocurrency into wallets controlled by the conspirators.

18. The conspirators laundered the stolen funds through virtual currency exchanges, online gambling websites, and converted the funds into other cryptocurrencies in order to conceal and disguise the nature, location, source, and ownership of the stolen funds.

OVERT ACTS

In furtherance of the conspiracy, and to achieve the objectives thereof, TREYTON DANIEL AUBUCHON, a/k/a "Aloel," Ruben Filipe Gabriel Martins, and their conspirators, committed and caused to be committed, the following overt acts, in the Eastern District of Pennsylvania and elsewhere:

1. On or about April 6, 2024, defendant TREYTON DANIEL AUBUCHON caused a call to be placed to Victim 1 from Google Voice Number 1142 purporting to be from a representative of a cryptocurrency exchange and informing Victim 1 that Victim 1's account had been compromised.

2. On or about April 6, 2024, during Victim 1's call with Google Voice Number 1142, Ruben Filipe Gabriel Martins caused a text message to be sent to Victim 1 from Google Voice Number 2627 which provided a link to spoofed website containing the name of the cryptocurrency exchange. The link provided to Victim 1 was one of the CryptoChameleon Phishing Panel domains.

3. On or about April 6, 2024, defendant TREYTON DANIEL AUBUCHON caused two text messages from Google Voice Number 1142 to be sent to Victim 1. The text messages provided a link to the same CryptoChameleon Phishing Panel domain referenced in paragraph 2 above.

4. On or about April 6, 2024, defendant TREYTON DANIEL AUBUCHON and Ruben Filipe Gabriel Martins caused Victim 1 to provide Victim 1's multi-factor authentication code from the cryptocurrency exchange to facilitate the transfer of Victim 1's funds to a supposedly secure wallet.

5. On or about April 6, 2024, defendant TREYTON DANIEL AUBUCHON and Ruben Filipe Gabriel Martins used the means of identification belonging to, and provided by, Victim 1 to access Victim 1's account without authorization and transferred Victim 1's funds to wallets controlled by the conspirators.

All in violation of Title 18, United States Code, Section 1349.

COUNT TWO

THE GRAND JURY FURTHER CHARGES THAT:

At all times material to this Indictment:

1. Paragraphs 1 through 10 and Overt Acts 1 through 5 of Count One of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.

The Scheme

2. From at least in or around April 2024 through at least in or about June 2025, defendant

**TREYTON DANIEL AUBUCHON,
a/k/a "Aloel,"**

together with, Ruben Filipe Gabriel Martins, charged elsewhere, knowingly devised and intended to devise a scheme to defraud Victim 1 and to obtain money and property by means of false and fraudulent pretenses, representations, and promises.

Manner and Means

3. Paragraphs 12 through 18 of Count One of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.

The Wire

4. On or about April 6, 2024, in the Eastern District of Pennsylvania and elsewhere, defendant

**TREYTON DANIEL AUBUCHON,
a/k/a "Aloel,"**

and Ruben Filipe Gabriel Martins, charged elsewhere, for the purpose of executing the scheme described above caused to be transmitted by means of wire communication in interstate and foreign commerce certain writings, signs, signals, pictures, and sounds, to wit, a Google voice call over

the Internet to Victim 1 falsely representing the caller to be from a cryptocurrency exchange in order to obtain access to Victim 1's account.

All in violation of Title 18, United States Code, Section 1343.

COUNT THREE

THE GRAND JURY FURTHER CHARGES THAT:

At all times material to this Indictment:

1. Paragraphs 1 through 10 and 12 through 18 and Overt Acts 1 through 5 of Count One of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.

2. On or about April 6, 2024, in the Eastern District of Pennsylvania and elsewhere, the defendant,

**TREYTON DANIEL AUBUCHON,
a/k/a "Aloel,"**

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, Victim 1, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is, wire fraud, knowing that the means of identification belonged to another real person, that is, Victim 1.

All in violation of Title 18, United States Code, Sections 1028A(a)(1), (c)(5).

NOTICE OF FORFEITURE

THE GRAND JURY FURTHER CHARGES THAT:

1. As a result of the violations of Title 18, United States Code, Sections 1343 and 1349, defendant

**TREYTON DANIEL AUBUCHON,
a/k/a "Aloel,"**

shall forfeit to the United States of America any property that constitutes, or is derived from, proceeds traceable to the commission of such offenses.

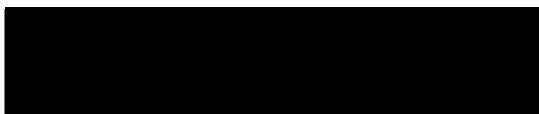
2. If any of the property subject to forfeiture, as a result of any act or omission of the defendant:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the Court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the property subject to forfeiture.

Pursuant to Title 28, United States Code, Section 2461(c) and Title 18, United States Code, Section 981(a)(1)(C).

A TRUE BILL:



GRAND JURY FOREPERSON

Salvatore L. Astolfi for
DAVID METCALF
UNITED STATES ATTORNEY

No. _____

UNITED STATES DISTRICT COURT

Eastern District of Pennsylvania

Criminal Division

THE UNITED STATES OF AMERICA

vs.

TREYTON DANIEL AUBUCHON
a/k/a "Aloel"

INDICTMENT

18 U.S.C. § 1349 (conspiracy to commit wire fraud – 1 count)
18 U.S.C. § 1343 (wire fraud – 1 count)
18 U.S.C. § 1028A (aggravated identity theft – 1 count)

[REDACTED]

Filed in open court this 18th day,
Of June A.D. 20 25

[REDACTED]

Bail, \$ _____